Тема 15. Мероприятия по защите информации. 2 часа

Проблема безопасности представляет собой как управленческую, так и техническую задачу и может оказывать значительное влияние на прогресс или регресс в использовании компьютерной технологии.

Защита осуществляется различными способами. Это может быть и физическая охрана, осуществляемая охранными предприятиями, и техническая защита с использованием специализированных средств и комплексов (например, защита от побочных электромагнитных излучений или от высокочастотных излучений). Защита конфиденциальной информации от несанкционированного доступа выполняется с использованием средств шифрования и без их применения.

Защита конфиденциальной информации в организации осуществляется путем проведения организационных, организационно-технических, инженерно-технических, программно-аппаратных и правовых мероприятий.

Организационные мероприятия предусматривают:

формирование и обеспечение функционирования системы информационной безопасности;

- организацию делопроизводства в соответствии с требованиями руководящих документов;
- использование для обработки информации защищенных систем и средств информатизации, а также технических и программных средств защиты, сертифицированных в установленном порядке;
- возможность использования информационных систем для подготовки документов конфиденциального характера только на учтенных установленным порядком съемных магнитных носителях и только при отключенных внешних линиях связи;
- организацию контроля за действиями персонала при проведении работ на объектах защиты организации;

- обучение персонала работе со служебной (конфиденциальной) информацией и др.

Основными *организационно-техническими* мероприятиями по защите информации являются:

- экспертиза деятельности организации в области защиты информации;
- обеспечение условий защиты информации при подготовке и реализации международных договоров и соглашений;
- аттестация объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями, составляющими служебную тайну;
- сертификация средств защиты информации, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам связи;
- разработка и внедрение технических решений и элементов защиты информации на всех этапах создания и эксплуатации объектов, систем и средств информатизации и связи;
- применение специальных методов, технических мер и средств защиты информации, исключающих перехват информации, передаваемой по каналам связи.

Для предотвращения угрозы утечки информации по техническим каналам проводятся следующие *инженерно-технические* мероприятия:

- предотвращение перехвата техническими средствами информации, передаваемой по каналам связи;
- выявление внедренных электронных устройств перехвата информации (закладных устройств);
- предотвращение утечки информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, электроакустических преобразований и др.

Программные (программно-аппаратные) мероприятия по предотвращению утечки информации предусматривают:

- исключение несанкционированного доступа к информации;
- предотвращение специальных воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;
- выявление внедренных программных или аппаратных "закладок";
- исключение перехвата информации техническими средствами;
- применение средств и способов защиты информации и контроля эффективности при обработке, хранении и передаче по каналам связи.

Правовые мероприятия – создание в организации нормативной правовой базы по информационной безопасности – предусматривают разработку на основе законодательных актов Российской Федерации необходимых руководящих и нормативно-методических документов, перечней охраняемых сведений, мер ответственности лиц за нарушение порядка работы с конфиденциальной информацией.

Перечень необходимых мер защиты конфиденциальной информации должен определяться дифференцированно в зависимости от конкретного объекта защиты информации и условий его расположения. Для примера можно рекомендовать следующие мероприятия по обеспечению информационной безопасности организации:

- подписание договора о неразглашении служащими, поставщиками и нанятыми по контракту работниками;
- регулярное создание резервных копий информации, хранящейся на мобильных компьютерах;
- регламентацию правил загрузки информации в мобильные компьютеры и правил использования информации;
- запрещение пользователям оставлять на рабочих местах памятки, содержащие идентификаторы и пароли доступа в корпоративную сеть;
- запрещение оставлять на корпусах мобильных компьютеров памятки, содержащие идентификаторы и пароли, применяемые для удаленного доступа;
- запрещение использовать доступ к Интернету в личных целях;

- обязательное применение пароля на загрузку компьютеров;
- создание классификации всех данных по категориям важности и усиление контроля над ограничением доступа в соответствии с ней;
- предотвращение доступа ко всем компьютерным системам по окончании рабочего дня;
- введение правил использования паролей доступа к файлам, содержащим информацию ограниченного доступа.

В результате созданная система обеспечения информационной безопасности должна обеспечить:

- пресечение попыток несанкционированного получения информации и доступа к управлению автоматизированной системой;
- пресечение и выявление попыток несанкционированной модификации информации;
- пресечение и выявление попыток уничтожения или подмены (фальсификации) информации;
- пресечение и выявление попыток несанкционированного распространения или нарушения информационной безопасности;
- ликвидацию последствий успешной реализации угроз информационной безопасности;
- выявление и нейтрализацию проявившихся и потенциально возможных дестабилизирующих факторов и каналов утечки информации;
- определение лиц, виновных в проявлении дестабилизирующих факторов и возникновении каналов утечки информации, и привлечение их к ответственности определенного вида (уголовной или административной).

Компьютерные вирусы и борьба с ними

Компьютерный вирус – это программа, обычно скрывающаяся внутри других программ, способная сама себя воспроизводить («размножаться») и приписывать себя к другим программам («заражать их») без ведома и согласия

пользователя, а также выполняющая ряд нежелательных действий на компьютере (проявление «болезни»).

Обычно вирусная программа создается специально для того, чтобы нарушить работу компьютеров или создать затруднения пользователю. Зараженные программы или электронные письма с вложенными зараженными файлами сами становятся носителями вируса и заражают другие объекты. Помимо заражения вирусы могут выполнять некоторые побочные действия, как безвредные (например, высвечивание на экране некоторого сообщения или воспроизведение какой-либо мелодии), так и злостные (уничтожение информации на носителях, замедление выполнения программ и т.д.). В начальной стадии заражения действие вируса может быть практически незаметно для пользователя. Однако через некоторое время одни программы перестают работать, другие начинают работать неправильно, скорость выполнения программ уменьшается, на экран выводятся посторонние сообщения и т.п. К этому времени, как правило, многие используемые программы оказываются зараженными, а возможно, и испорченными. Велика вероятность того, что в процессе работы через локальную сеть (при ее наличии) или с помощью электронной почты вирус распространится на другие компьютеры. Такой спонтанный процесс распространения вирусов называют «эпидемией».

При заражении компьютера вирусом важно его своевременно обнаружить. Для этого следует знать основные признаки их проявления, к которым можно отнести следующие:

- участившиеся перезагрузки или зависание компьютера;
- замедленные загрузка и выполнение программ;
- мигание лампочки дисковода, когда не должны происходить операции записи-чтения;
- изменение размеров выполняемых программ;
- уменьшение объема основной доступной памяти.

Следует отметить, что вышеперечисленные явления не обязательно вызываются присутствием вируса, они могут быть следствием других причин.

Именно поэтому всегда затруднена правильная диагностика состояния компьютера.

В целях защиты компьютеров от заражения вирусами рекомендуется:

- оснастить свой компьютер современными антивирусными программами (например, DrWeb, AVP, McAfee, NAV или другими) и постоянно обновлять их версии;
- регулярно создавать резервные копии важных файлов и системных областей жестких дисков;
- периодически проверять на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков;
- перед считыванием с дискет информации, записанной на других компьютерах, всегда проверять эти дискеты на отсутствие вирусов, запуская антивирусные программы своего компьютера до чтения содержания дискет;
- при переносе на свой компьютер файлов в архивированном виде проверять их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;
- всегда защищать свои дискеты от записи при работе на других компьютерах, если на них не будет проводиться запись информации.